Welcome to session II

Latest trends and innovations resulting from ITEA Cyber Security projects
CyberFactory#1
Project Ambition
Adrien Bécue,
Airbus Cybersecurity
31 May 2016 - Cyberattack on a German steel-mill Factory

Attack reports by BSI and SANS Institute

Attacker profile
- State sponsored
- Skilled in IT
- Skilled in ICS
- Aiming at physical damage

Attack story
- Spear phishing
- Credentials theft
- Hack into office network
- Infect Production mgmt SW
- Access industrial Ntwk
- Control Blast furnace
- Destroy HMs
- Prevent safety shut down

Damages
- Plant damaged by molten metal heated to thousands °
- Production loss
- Reputational damage
Industry 4.0 Transformation

**Industry 4.0:** leveraging 3D printing, cobotics, IoT, Cloud, Artificial Intelligence
> towards agile and highly automated techniques for networked manufacturing of customizable products
Industrial cyber-risk – Tomorrow?

- Autonomous robot kills a worker! Adversarial machine learning suspected...
- Military secret stolen in weapon factory! Rogue device placed by contractor leaked rocket warhead design data...
- 387 Aircraft stuck on the ground Undetected production defaults on Avionics...
CyberFactory#1 Project value chain

**Users**
- U1 - Transportation systems
- U2 - Textile industry
- U3 - Consumer Electronics
- U4 - Machine fabrication

**Suppliers**
- S1 - Robotics & Automation
- S2 - IIoT & M2M Communication
- S3 - SCADA, ERP & Supply Chain Mgmt
- S4 - Security & Safety

**Researchers**
- R1 - Cyber-physical system engineering
- R2 - Data science & artificial intelligence
- R3 - Economics & Social Sciences
- R4 - Virtualization, Modelling & Simulation
CyberFactory#1 Project key capabilities

**Technical dimension**
- CAP31 - CPS Modelling & Digital Twins
- CAP32 - Factory ecosystem modelling
- CAP33 - Human behavior modelling
- CAP34 - Factory SoS modelling

**Economical dimension**
- CAP41 - Real-time sensing & tracking
- CAP42 - Manufacturing data-lake exploitation
- CAP43 - Human/Machine optimization
- CAP44 - Distributed Manufacturing

**Human dimension**
- CAP51 - Human/Machine access & trust mgmt
- CAP52 - Adversarial/Robust learning
- CAP53 - Human/Machine behavior watch
- CAP54 - Cyber-resilience mechanisms

**Societal dimension**
Digital Twin Market
-USD 3.8 Billion in 2019
-USD 35 Billion by 2025
-CAGR of 37.8%

Industry 4.0 Market
-USD 66.67 Billion in 2016
-USD 152.31 Billion by 2022
-CAGR of 14.72%

ICS Security Market
-USD 10.24 Billion in 2017
-USD 13.88 Billion by 2022
-CAGR of 6.3%
Thank you!

https://www.cyberfactory-1.org/en/home/
adrien.becue@airbus.com
DEFRAUDify
Detecting Fraudulent Activities on the internet
ITEA Cyber Security Day (Jan 15th 2021)
Freek Bomhof (TNO)
Project background

- The internet is a wonderful technology…
- It can be used for good… and for bad
- Detecting fraud is not only a challenge for Law Enforcement Agencies
Project concept

Information on fraudulent activities can be found in many places:
The innovation

Comprehensive analysis
▪ Combining existing sources
▪ Adding sources that had not yet been included before
▪ Cross media analytics

Active monitoring
▪ Probing the adversaries to elicit behaviour
▪ Honeypots, autonomous agents

Privacy regulations
▪ Pseudonymization while scraping, not storing personal identifiable information
▪ GDPR compliant

Ecosystem of microservices
▪ Not one monolithic platform
▪ But interoperable and flexibly combinable tools
Use cases & partners

- **Netherlands**
  - Detect money laundering VC <> real currencies
  - Strategic monitoring company fraud

- **Turkey**
  - Managed Security Service Providers & Cyber Defence

- **Romania**
  - Detect virtual currency fraud

TNO, Slimmer, Web-IQ, Cointel, Almende, bunq, Target, TU/e, Hoffmann

IntelProbe

BEIA
PARFAIT
Personal Data Protection Framework for IoT
ITEA Cyber Security Day 2021
Isil Ozkan, Turkcell Teknoloji
Needs and Proposition

Emerging Needs

Security & Privacy
- Security is the most important barrier on the growth of Internet of Things applications
- Device security
- Security & management of personal data

Interoperability
- Lack of structures for interoperability increases complexity of service and application development in Internet of Things
- Complex service and application development increases production and maintenance costs

PARFAIT aims at providing a integrated solution in the Internet of Things domain

<table>
<thead>
<tr>
<th>PARFAIT</th>
<th>Application/Service Development</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security/Privacy Implementation</td>
<td></td>
</tr>
<tr>
<td>Connectivity of Things</td>
<td>Specialized Hardware</td>
</tr>
<tr>
<td>Data Management</td>
<td>AI/ML Implementations</td>
</tr>
</tbody>
</table>
Objectives of Parfait
Personal Data Protection Framework for IoT

PARFAIT project’s main goal is to develop a platform for protecting personal data in Internet of Things applications

NEED: Internet of Things (IoT) related data security issues often undermine privacy and trust. Interoperability increases the complexity of services and costs of production, while also multiplying vulnerabilities and security needs.

Currently, interoperability, privacy and security have limited accepted standards in the IoT domain.

PROPOSITION: The ITEA project PARFAIT aims to develop a framework for protecting personal data in IoT applications, opening the way to connected ecosystems.

It defines indistinct aspects of the IoT domain, interoperability and privacy, by implementing rules, guidelines and methodologies.

BENEFITS: The global security framework will increase the deployment of large-scale, global business applications and will make IoT provide better communication, reduced costs and more access to services.
Consortium Structure

France
- NXP Semiconductors
- Thales
- PERTIMM
- Softeam Cadextan
- University of Burgundy
- University of La Rochelle

Romania
- BEIA Consult International
- Societatea de Inginerie Sisteme SIS SA

Turkey
- Ericsson Ar-Ge
- Turkcell Teknoloji
- Turkgen

Effort: 75 [PY]
Cost: 5.5 [kEuro]
Parfait Architecture System with Partner Overview

**SMART HOTEL**

- Security/Privacy Aspects
  - Thales
  - Pertimm
  - Softeam
  - UoB
  - BEIA

- Cloud layer (Servers)
  - TurkGen
  - UoLR
  - Personal data management

- Network layer
  - OPC
  - MQTT
  - NFC
  - Zigbee
  - Wi-fi
  - Cellular

- Hardware layer
  - NXP
  - SIS

**SMART HOME**

- Communication/Network Aspects
  - Turkcell Technology
  - Turkcell Technology

- Consortium members:
  - French Partners
  - Romanian Partners
  - Turkish Partners
  - Thales
  - Ericsson Turkey

**French Partners**
- NXP
- UoB

**Romanian Partners**
- BEIA

**Turkish Partners**
- SIS
- Thales
- Turkcell Technology
- Turkcell Technology
- Ericsson Turkey
Technology And Market Value Chain

APPLICATION SPACE
- Smart Home Application
- Smart Hotel Application

SERVICE FRAMEWORK
- Smart Domain Framework
- Personal Data Management Services

PRIVACY AND SECURITY FRAMEWORK
- Secure Interfaces for Hardware Management
- Partial and Full Anonymization
- Authentication Libraries
- Data Storage Services
- Encryption & Decryption
- File management

EXTERNAL SERVICES
- NFC Tags
- Secure Elements
- MCUs
- Zigbee & BLE
- IoT Integration
- Configuration
- Visualization dashboard
- Data Storage Services

Hardware Providers
- NXP
- Thales

Tool & Software Providers
- Thales
- Pertimm
- Softeam
- SIS
- Turkgen
- Ericsson
- Uni. La Rochelle

Service & Application Providers
- Turkcell
- SIS
- BEIA
- Ericsson
- Uni. Of Burgundy
- Uni. La Rochelle

Customers
- Business Customers
- End User Customers

<<Provide hardware components>>
- Intelligence modules
- Semantic services
- API for smart token
- Connectivity modules
<<Provide software infrastructure>>
- Smart Home
- Smart Hotel
<<Provides services to customers>>
## Current Market Trends – IoT Platforms

### Key IoT Trends and Technologies

<table>
<thead>
<tr>
<th>AI</th>
<th>Social/legal/ethical IoT</th>
<th>Infonomics and data broking</th>
<th>Intelligent IoT mesh</th>
<th>IoT governance</th>
</tr>
</thead>
<tbody>
<tr>
<td>Pertimm Turkgen, BEIA</td>
<td>Thales Softeam, UoLR</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Sensor innovation</th>
<th>Trusted hardware and OS</th>
<th>Novel IoT user experiences</th>
<th>Silicon chip innovation</th>
<th>New wireless networks</th>
</tr>
</thead>
<tbody>
<tr>
<td>NXP, Thales</td>
<td></td>
<td>TTECH, SIS, UoB, UoLR</td>
<td></td>
<td>NXP, Thales, Ericsson TR, BEIA, SIS</td>
</tr>
</tbody>
</table>
Standardization: FIDO

- The FIDO Alliance (www.fidoalliance.org) is an open industry association with a focused mission: **authentication standards to help reduce the world’s over-reliance on passwords**
- Simpler for consumers to use, and easier for service providers to deploy and manage
- +240 Members: major on-line service providers, banks, Operating System providers, device security vendors, …
- Has published three sets of specifications known as FIDO2
- Creation of IoT Technical Working Group (IoT TWG): develop use cases, target architectures and specifications

**UAF: Universal Authentication Framework**
Multi Factor authentication (possession + knowledge/inherence)

**U2F: Universal 2\(^{nd}\) Factor**
Login & Password + possession factor

**FIDO 2: Brings FIDO support to the web browser, to Windows 10 and to Android 7**

**WebAuthn: standard APIs**

**CTAP (Client to Authenticator Protocol):**
### FIDO Certified Authenticator Levels

#### SAMPLE DEVICE HARDWARE & SOFTWARE REQUIREMENTS

<table>
<thead>
<tr>
<th>Requirement</th>
<th>Level</th>
<th>Defense Against</th>
</tr>
</thead>
<tbody>
<tr>
<td>Protection against chip fault injection and invasive attacks</td>
<td>L3+</td>
<td>Chip level attacks on captured devices</td>
</tr>
<tr>
<td>Circuit board potting, package on package memory, encrypted RAM...</td>
<td>L3</td>
<td>Circuit board attacks on captured devices</td>
</tr>
<tr>
<td>Device must support allowed Restricted Operating Environment (ROE) (e.g., TEE, Secure Element...), or intrinsically be an ROE (e.g., a USB token or Smart Card...)</td>
<td>L2+</td>
<td>Device OS compromise</td>
</tr>
<tr>
<td>Any device HW or SW</td>
<td>L1+</td>
<td>White Box Cryptography to defend against OS compromise</td>
</tr>
<tr>
<td></td>
<td>L1</td>
<td>Phishing, server credential breaches and MiTM attacks (better than passwords)</td>
</tr>
</tbody>
</table>

#### FIDO AUTHENTICATOR CERTIFICATION EXAMPLES

- **L3+**
  - USB U2F Token built on a CC-certified Secure Element
  - L3+ U2F Token built on a basic simple CPU, OS is certified. Good physical anti-tampering enclosure
  - Certification: L3
  - L2+ U2F token running on a certified TEE with POP memory
  - Certification: L3

- **L3**
  - USB U2F Token built on a basic simple CPU, OS is certified. Good physical anti-tampering enclosure
  - FIDO2 making use of the Android keystore: Keystore runs in a TEE that is certified at L2+ Certification: L2
  - L2: UAF implemented in a TA running on a certified TEE with POP memory
  - Certification: L3

- **L2+**
  - L1+ U2F in downloadable app using white box and other techniques
  - FIDO2 making use of the Android keystore
  - Keystore is not certified Certification: L1
  - L1+ U2F in downloadable app using white box and other techniques
  - Certification: L1

- **L2**
  - Downloaded app making use of Touch ID on iOS Certification: L1

- **L1+**
  - L1+ U2F in downloadable app using white box and other techniques Certification: L1

- **L1**
  - Downloaded app making use of Touch ID on iOS Certification: L1

ITEA Cyber Security Day, 15 Jan
Dissemination & Exploitation Overview

Dissemination

- Recruitment: 22 employees
- Patents: 2
- Project Presence in events: 12
- Technical Presentations: 19
- Publications: 17
- Web Presentations: 12

Product/Service/System/Library/Enhancement

- BiP User interface for smarthome
- IoT Manager Enhancements
- SmartHome Chatbot
- FIDO Implementation for IoT
- Secure Chipsets in IoT
- NFS/SE combo
- eIDAS/FIDO Token Enhancements
- PIMS for IoT
- Multilingual NLP platform
- Development of SmartHotel platform (TRL4)
- Token based lightweight authentication
- Secure reservation system
- Bid-Aware Privacy-Preserving data collection in IoT
- OPC Interface in IoT Gateway
- Gateway for secure IoT Data Collection
- Smart Lock/Door
Parfait Platform completed with software and hardware outputs in the IoT domain. Collaborative architecture: Flexibility, Modularity, Reusability with Security Applications on Smart Home / Smart Hotel with exploitation opportunity.
Thank you
Project start: September 2018
Project end: March 2022
Project leader: Andries Stam, Almende BV
andries@almende.org
Till Witt, Consider IT GmbH
till.witt@nxp.com
Website: scratch-itea3.eu
Problem and State-of-the-Art

- Lack of support for Security in DevOps, especially for SMEs in the IoT domain
- Heterogeneous tool landscape, lack of integrated approach and practical guidelines
Project Objectives

• **Secure DevOps Toolkit**
  • Existing and newly created tools for the entire SecDevOps chain
  • Aimed at SMEs to address the security of their IoT products and services

• **Secure DevOps Methodology**
  • Enable SMEs in the IoT domain to systematically achieve security standards
  • Guidelines to help SMEs to find appropriate tools and ways of working
  • Best practices for all DevOps phases and an SDK blueprint repository

• **Secure DevOps Knowledge Base**
  • SotA Knowledge Base for Secure DevOps for IoT focused on SME communities
  • Currently 5 standardization efforts included

• **Improved applications for 4 use case domains:**
  • Connected Retail, Police, Smart Grids and Smart Machinery
Online Survey: https://scratch-itea3.eu/survey/
Thank you for your attention
STACK: Smart, Attack-resistant IoT Networks

- Thiemo Voigt
  RISE Computer Science, Sweden
STACK’s Participants

- Sweden: ASSA ABLOY, Husqvarna, LumenRadio, RISE
- Romania: BEIA Consult International
- South Korea: Korea Electronics Technology Institute (KETI), Security Platform, Seoul National University, Yonsei University

- Started in December 2020
STACK’s Main Goal

• Enable a new class of critical Internet of IoT applications that:
  • Operate and provide quality of service even in harsh or malicious conditions
• Achieved by
  • Attack detection and mitigation on IoT devices / Edge
  • More robust IoT communication
• Strongly required when digitizing products
STACK’s Applications

- Commercial partners have critical applications
- Mesh networks of critical IoT devices
Vulnerability of Low-Power IoT

- Resource constraints
  - Low-power radio communication (DoS)
  - New attacks, e.g., on battery
- Systems software not as secure
  - Often specialized, non-commercial operating systems
- No commercial tools for e.g. intrusion detection
STACK’s Main Technical Work Items

Smart Attack Detection and Mitigation

- Attack detection at several layers including AI-based malicious network activity detection
- Sensor testing and identification
- Attack mitigation
STACK’s Main Technical Work Items

Attack Prevention

• Protocols and mechanisms for predictable networking
• Network security support
• Hardware support for attack prevention
Thank you!